WHEN IS THE COMMUTANT OF A BOL LOOP A SUBLOOP?

MICHAEL K. KINYON, J. D. PHILLIPS, AND PETR VOJTĚCHOVSKÝ

Abstract. A left Bol loop is a loop satisfying $x(y(xz)) = (x(yx))z$. The commutant of a loop is the set of elements which commute with all elements of the loop. In a finite Bol loop of odd order or of order $2k$, k odd, the commutant is a subloop. We investigate conditions under which the commutant of a Bol loop is not a subloop. In a finite Bol loop of order relatively prime to 3, the commutant generates an abelian group of order dividing the order of the loop. This generalizes a well-known result for Moufang loops. After describing all extensions of a loop K such that K is in the left and middle nuclei of the resulting loop, we show how to construct classes of Bol loops with non-subloop commutant. In particular, we obtain all Bol loops of order 16 with non-subloop commutant.

1. Introduction

A *loop* $(Q, \cdot)$ is a set Q with a binary operation $\cdot$ such that there is a neutral element $1 \in Q$ satisfying $1 \cdot x = x \cdot 1 = x$ for all $x \in Q$, and such that for each a, $b \in Q$ the equations $a \cdot x = b$ and $y \cdot a = b$ have unique solutions x, $y \in Q$. We write xy instead of $x \cdot y$, and reserve $\cdot$ to have lower priority than juxtaposition among factors to be multiplied—for instance, $x \cdot yz$ stands for $x(yz)$.

The *commutant* (also known as the *centrum*, *Moufang center* or *semicenter*) of a loop Q is the set

$$C(Q) = \{c \in Q \,|\, cx = xc \text{ for every } x \in Q\}.$$

In a group, or even a Moufang loop, the commutant is a subloop, but this does not need to be the case in general. When Q is a loop and $C(Q)$ is not a subloop of Q, we say that Q *has a non-subloop commutant.*

Given an element a of a loop Q, we denote by L_a the left translation of Q by a, *i.e.*, $bL_a = ab$. Similarly, R_a is the right translation $bR_a = ba$. The commutant is obviously characterized as $C(Q) = \{c \in Q \,|\, L_c = R_c\}$. The permutation group $\langle L_a, R_a \,|\, a \in Q\rangle$ is known as the *multiplication group* of Q, and will be denoted by $\mathrm{Mlt}(Q)$. We also use the notations $R : Q \to \mathrm{Mlt}(Q); a \mapsto R_a$ and $L : Q \to \mathrm{Mlt}(Q); a \mapsto L_a$.

A loop is *left Bol* if it satisfies

$$x(y \cdot xz) = (x \cdot yx)z \qquad \text{(Bol)}$$

for all x, y, z, or equivalently, if $L_xL_yL_x = L_{x\cdot yx}$ for all x, y. Right Bol loops are defined by the mirror of (Bol). We will consider only left Bol loops in this paper, and henceforth refer to them simply as Bol loops. Note that much of the literature

Date: February 2, 2008.

1991 *Mathematics Subject Classification.* 20N05.

Key words and phrases. Bol loop, commutant, extension of loops.

on Bol loops (*e.g.*, [14]) considers right Bol loops, and hence results need to be translated appropriately.

The main purposes of this paper are to introduce general constructions of Bol loops with non-subloop commutants, and to shed light on the structure of the commutant of a Bol loop, of the subloop generated by the commutant, and of the subgroup $\langle L_c \,|\, c \in C(Q)\rangle$ of $\mathrm{Mlt}(Q)$.

The commutant of a finite Bol loop of odd order is a subloop [7]. In Theorem 2.8, we show that the commutant of a finite Bol loop of order $2k$, k odd, is a subloop. Thus finite Bol loops with non-subloop commutant have order divisible by 4 (Corollary 2.9). When the commutant of a Bol loop is a subloop, it is a commutative Moufang loop. In case Q is a Bol loop with a non-subloop commutant, it is natural to consider the structure of the subloop $\langle C(Q)\rangle$. In Corollary 3.6, we show that if Q is finite of order relatively prime to 3, then $\langle C(Q)\rangle$ is an abelian group of order dividing $|Q|$. This generalizes a well-known result about commutants of Moufang loops. We then turn to constructions. In §4, we describe all extensions Q of a group K such that K is contained in the left and middle nuclei of the resulting loop. In the next two sections, we specialize this to construct examples of Bol loops with non-subloop commutants. In §5, we consider the special case of a semidirect product (split extension), and in §6, we consider the special case where the action of Q/K on K is trivial. When we restrict to low orders, the two constructions give 20 of the 21 known Bol loops of order less than or equal to 16 with non-subloop commutant. We finish with another construction which yields the remaining such loop.

We conclude this introduction with a review of some basic facts regarding loops in general and Bol loops in particular. The standard references [1, 13] provide adequate general background in loop theory, while the latter reference, [5, Chap. VI], and [14] give specific details regarding Bol loops.

For a loop Q, the following subgroups (associative subloops) are of interest:

- the *left nucleus* $N_\lambda(Q) = \{a \in Q \,|\, a \cdot xy = ax \cdot y, \forall x, y \in Q\}$
- the *middle nucleus* $N_\mu(Q) = \{a \in Q \,|\, x \cdot ay = xa \cdot y, \forall x, y \in Q\}$
- the *right nucleus* $N_\rho(Q) = \{a \in Q \,|\, x \cdot ya = xy \cdot a, \forall x, y \in Q\}$
- the *nucleus* $N(Q) = N_\lambda(Q) \cap N_\mu(Q) \cap N_\rho(Q)$
- the *center* $Z(Q) = N(Q) \cap C(Q)$

The center is a normal subloop. In a Bol loop Q, the left and middle nuclei coincide, $N_\lambda(Q) = N_\mu(Q)$, and we shall just refer to this as the left nucleus. The left nucleus of a Bol loop is a normal subloop, but does not necessarily coincide with the right nucleus, nor is the right nucleus necessarily normal. In addition, $Z(Q) = C(Q) \cap N_\lambda(Q)$. Indeed, for $c \in C(Q) \cap N_\lambda(Q)$ and $x, y \in Q$, $xy \cdot c = c \cdot xy = cx \cdot y = xc \cdot y = x \cdot cy = x \cdot yc$. Thus $c \in N_\rho(Q)$ and so $c \in Z(Q)$.

Let Q be a Bol loop. Then Q is *power-associative*, that is, for each $x \in Q$, the subloop $\langle x\rangle$ generated by x is a subgroup. In particular, there exists $x^{-1} \in Q$ such that $xx^{-1} = x^{-1}x = 1$. In addition, Q is *left power alternative*, that is,

$$x^m \cdot x^n y = x^{m+n} y \tag{LPA}$$

for all integers m, n. Equivalently, $L_x^m = L_{x^m}$ for every integer m. An element $a \in Q$ is said to be *right power alternative* if $R_a^m = R_{a^m}$ for every integer m. Not every element of a nonMoufang Bol loop Q is right power alternative.

For a Bol loop Q, a subset S is a subloop if and only if it is closed under both multiplication and inversion. Indeed, if $a, b \in S$, then the unique solutions of the equations $ax = b$ and $ya = b$ are $x = a^{-1}b \in S$ and $y = a^{-1}(ab \cdot a^{-1}) \in S$, respectively.

Lemma 1.1. *Let Q be a finite loop, and let $S \subseteq Q$ be a subloop.*

(i) *If $R|_S : S \to \mathrm{Mlt}(Q)$ is a homomorphism, then $|S|$ divides $|Q|$.*
(ii) *If $L|_S : S \to \mathrm{Mlt}(Q)$ is a homomorphism, then $|S|$ divides $|Q|$.*

Proof. Fix $x, y \in Q$, and suppose $xS \cap yS \neq \emptyset$. Then there exist $s_1, s_2 \in S$ such that $xs_1 = ys_2$, and so $x = yR_{s_2}R_{s_1}^{-1} = yR_{s_3} = ys_3$ where $s_3s_1 = s_2$. Thus for all $s \in S$, $xs = yR_{s_3}R_s = y \cdot s_3s \in yS$, and so $xS \subseteq yS$. The other inclusion follows similarly, and so $xS = yS$. Therefore $\{xS \mid x \in Q\}$ is a partition of Q. This establishes (i), and the proof of (ii) is similar, using left cosets instead of right cosets. □

Corollary 1.2. *Let Q be a finite loop.*

(i) *If S is a subgroup of $N_\rho(Q)$, then $|S|$ divides $|Q|$.*
(ii) *If S is a subgroup of $N_\lambda(Q)$, then $|S|$ divides $|Q|$.*

If, in addition, Q is a Bol loop, then for each $x \in Q$, $|\langle x \rangle|$ divides $|Q|$.

Proof. Parts (i) and (ii) follow from the respective parts of Lemma 1.1. The remaining assertion is well-known [13, 14], and follows from (LPA). □

It is not known if the order of an arbitrary subloop of a finite Bol loop divides the order of Q.

2. Structure of the Commutant

Throughout this section, let Q denote a Bol loop with commutant $C(Q)$.

Lemma 2.1. *If $a \in C(Q)$, then:*

(i) $\langle a \rangle \subset C(Q)$,
(ii) *a is right power alternative.*

In addition, if $b \in C(Q)$, then:

(iii) $a^2b \in C(Q)$,
(iv) $a^kb^\ell \cdot a^mb^n = a^{k+m}b^{\ell+n}$ *for all integers k, ℓ, m, n.*

Proof. For (i) and (iii), see Lemmas 2.2 and 2.1 of [7]. Part (ii) follows from (i) and (LPA). Let us prove (iv):

$$\begin{aligned} a^kb^\ell \cdot a^mb^n &= a^{-m} \cdot a^m(a^kb^\ell \cdot a^mb^n) = a^{-m}[a^m(a^kb^\ell \cdot a^m) \cdot b^n] \\ &= a^{-m} \cdot (a^{2m} \cdot a^kb^\ell)b^n = a^{-m}(a^{k+2m}b^\ell \cdot b^n) \\ &= a^{-m} \cdot a^{k+2m}b^{\ell+n} = a^{k+m}b^{\ell+n} \end{aligned}$$

using (LPA), (Bol), (i), (LPA) twice, (ii), and (LPA) once more. □

Part (i) of the lemma immediately implies the following.

Corollary 2.2. *$C(Q)$ is a subloop if and only if it is closed under multiplication.*

We introduce here some useful notation. For an integer $n > 1$, let

$$C_n(Q) := \{c \in C(Q) \,|\, c \text{ has finite order relatively prime to } n\}.$$

Obviously, if $m > 1$ divides n, $C_n(Q) \subseteq C_m(Q)$.

Lemma 2.3. *Let $n > 1$ be an integer.*

(i) *If $a \in C_n(Q)$, then $\langle a \rangle \subseteq C_n(Q)$.*
(ii) *If $a, b \in C_n(Q)$, then ab has order relatively prime to n.*
(iii) *If $a, b \in C_n(Q)$, then $a^2 b \in C_n(Q)$.*
(iv) *If $m > 1$ divides n, and if $C_m(Q)$ is a subloop, then $C_n(Q)$ is a subloop.*

Proof. Part (i) is immediate from Lemma 2.1(i), part (ii) follows from Lemma 2.1(iv), and (iii) follows from (ii) and Lemma 2.1(iii). Finally, (iv) follows from (ii) and $C_n(Q) \subseteq C_m(Q)$. □

The following is a mild generalization of the main result of [7].

Corollary 2.4. *For each integer $m > 0$, $C_{2m}(Q)$ is a subloop of Q.*

Proof. By Lemma 2.3(iv), it is enough to show that $C_2(Q)$ is a subloop. By Lemma 2.3(i), $C_2(Q)$ is closed under inversion. If $a, b \in C_2(Q)$, then by Lemma 2.3(i), there exists $c \in C_2(Q)$ such that $c^2 = a$, and so $ab = c^2 b \in C_2(Q)$, using Lemma 2.3(iii). □

Lemma 2.5. *For $c \in C(Q)$, $c^2 \in N_\lambda(Q)$ if and only if $c \in N_\rho(Q)$.*

Proof. For x, $y \in Q$, we compute

$$c^2 \cdot xy = c(c \cdot xy) = (xy \cdot c)c \tag{2.1}$$

and

$$c^2 x \cdot y = (c \cdot xc)y = c(x \cdot cy) = (x \cdot yc)c. \tag{2.2}$$

Now $c^2 \in N_\lambda(Q)$ iff the left hand sides of (2.1) and (2.2) are equal, while $c \in N_\rho(Q)$ iff the right hand sides are equal. The result follows. □

Corollary 2.6. *If $C(Q) = C_2(Q)$, then $Z(Q) = C(Q) \cap N_\rho(Q)$.*

Proof. In this case, the lemma gives $C(Q) \cap N_\rho(Q) = C(Q) \cap N_\lambda(Q) = Z(Q)$. □

Corollary 2.7. *If $S \subseteq \{c \in C(Q) \,|\, c^2 \in N_\lambda(Q)\}$, then S generates an abelian subgroup of $N_\rho(Q)$.*

Theorem 2.8. *Let Q be a finite Bol loop of order $2k$ where k is odd. Then $C(Q)$ is a subloop of Q.*

Proof. If $C(Q) = C_2(Q)$, then the result follows from Corollary 2.4. Thus assume $1 \neq a \in C(Q)$ has order 2. Fix $b \in C(Q)$ of even order $2m$ where m divides k. Then b^m has order 2. If $b^m \neq a$, then by Corollary 2.7, $\langle a, b^m \rangle$ is an abelian subgroup of $N_\rho(Q)$ of order 4. But then by Corollary 1.2(i), 4 divides $|Q|$, a contradiction. Thus $b^m = a$. Set $c = b^{m+1}$ and note that $b = ac$. Hence $c^m = a^m b^m = aa = 1$.

Summarizing, every element of $C(Q)$ can be written uniquely in the form $a^i c$ where $i \in \{0, 1\}$ and where $c \in C_2(Q)$. For $c_1, c_2 \in C_2(Q)$, $c_1 c_2 \in C_2(Q)$ (Corollary

2.4), and $a^i c_1 \cdot a^j c_2 = a^{i+j} \cdot c_1 c_2$, $i, j \in \{0, 1\}$, by Lemma 2.1(iv). Thus $C(Q)$ is closed under multiplication, and so by Corollary 2.2, it is a subloop. □

Corollary 2.9. *If Q is a finite Bol loop with non-subloop commutant, then 4 divides $|Q|$.*

In Proposition 5.8, we will show that for each integer $n > 2$, there exists a Bol loop of order $4n$ with non-subloop commutant.

3. Commutant elements of order prime to 3

We now proceed to show that in a Bol loop, commutant elements of order relatively prime to 3 generate an abelian group. This generalizes the well-known result that in a Moufang loop, commutant elements of order relatively prime to 3 lie in the center. There are nonassociative commutative Moufang loops, the smallest being of order 81, and so the assumptions on the orders of elements or of loops are necessary.

We adopt the following convention: for elements $a_1, a_2, \ldots, a_n$ of a loop Q, $a_1 a_2 \cdots a_n$ will denote the left-associated product $(\cdots(a_1 a_2)\cdots)a_n$.

Theorem 3.1. *Let Q be a Bol loop, let $A \subseteq C(Q)$, and suppose that for each $a, b \in A$, $R_a R_b = R_{ab}$. Then the subloop $\langle A \rangle$ is an abelian subgroup of Q, and $R|_{\langle A \rangle} : \langle A \rangle \to \mathrm{Mlt}(Q)$ is a homomorphism.*

If, in addition, Q is finite, then $|\langle A \rangle|$ divides $|Q|$.

Proof. Since $R_a R_b = R_b R_a$ for all $a, b \in A$, we may freely rearrange products of right translations from A. For $n > 0$, let $a_1, \ldots, a_n \in A$. We will verify

$$R_{a_1 a_2 \cdots a_n} = R_{a_1} R_{a_2} \cdots R_{a_n} \tag{3.1}$$

by induction on n. By hypothesis, (3.1) holds for $1 \le n \le 2$. Suppose $n > 2$ and that (3.1) holds for $n - 1$. Then

$$\begin{aligned} a_{n-1} \cdot [x R_{a_1} \cdots R_{a_{n-2}} R_{a_{n-1}} R_{a_n}] &= a_{n-1} [x R_{a_1} \cdots R_{a_{n-2}} \cdot a_{n-1} a_n] \\ &= \big(a_{n-1} \cdot x R_{a_1} \cdots R_{a_{n-2}} R_{a_{n-1}}\big)\, a_n \\ &= \big(a_{n-1} \cdot x R_{a_1 \cdots a_{n-2} a_{n-1}}\big)\, a_n \\ &= (a_{n-1} \cdot x[a_{n-1} \cdot (a_1 \cdots a_{n-2})])\, a_n \\ &= [(a_{n-1} \cdot x a_{n-1}) \cdot (a_1 \cdots a_{n-2})] a_n \\ &= (a_{n-1} \cdot x a_{n-1})(a_1 \cdots a_{n-2} a_n) \\ &= a_{n-1} \cdot x[a_{n-1} \cdot (a_1 \cdots a_{n-2} a_n)] \\ &= a_{n-1} \cdot x(a_1 \cdots a_{n-2} a_{n-1} a_n). \end{aligned}$$

Here we are using, in succession, $R_{a_{n-1}} R_{a_n} = R_{a_{n-1} a_n}$, (Bol), the induction hypothesis, $a_{n-1} \in C(Q)$, (Bol) again, the induction hypothesis again, (Bol) once more, $a_{n-1} \in C(Q)$ again, and $R_{a_n} R_{a_{n-1}} = R_{a_{n-1}} R_{a_n}$. Cancelling a_{n-1}, we obtain (3.1) for n.

Since $a_1a_2\cdots a_n = 1R_{a_1}R_{a_2}\cdots R_{a_n}$, and since $R_{a_i}R_{a_j} = R_{a_j}R_{a_i}$ for all i, j, it follows that the expression $a_1a_2\cdots a_n$ is invariant under all reassociations and rearrangements. Thus $\langle A\rangle$ is an abelian group, and the homomorphism assertion follows from (3.1).

The remaining claim follows from Lemma 1.1(i). □

Lemma 3.2. *Let Q be a Bol loop, and suppose $a, b \in C(Q)$ satisfy $R_aR_b = R_bR_a$. Then $R_aR_b = R_{ab}$.*

Proof. We compute

$$a(xa \cdot b) = (xa \cdot b)a = (xa \cdot a)b = (a \cdot xa)b = a(x \cdot ab),$$

using (Bol) in the last step. Cancelling a, we have the desired result. □

Lemma 3.3. *Let Q be a Bol loop, and let a, b, $c \in C(Q)$. Then:*

(i) *for all $x \in Q$, $xb \cdot a^3 = xa^3 \cdot b = x \cdot a^3b$,*

(ii) *for all $x \in Q$, $x^3a \cdot b = x^3b \cdot a = x^3 \cdot ab$.*

Proof. By Lemma 2.1, $a(b \cdot ax) = (a \cdot ba)x = a^2b \cdot x = x \cdot a^2b$. Thus $a^3(ax \cdot b) = a^3(b \cdot ax) = a^2 \cdot a(b \cdot ax) = a^2(x \cdot a^2b) = (a^2 \cdot xa^2)b = (a^3 \cdot ax)b$. Replacing x with $a^{-1}x$ and using $a^3, b \in C(Q)$, we have the first equality of (i). The second equality follows from Lemma 3.2.

Next, we compute $a \cdot x^2a = a^3 \cdot a^{-2}(x \cdot xa) = a^3(a^{-1} \cdot (x \cdot ax)a^{-1})$, and so $a(x^2 \cdot ab) = (a \cdot x^2a)b = a^3(a^{-1} \cdot (x \cdot ax)a^{-1}) \cdot b = a^3 \cdot (a^{-1} \cdot (x \cdot ax)a^{-1})b = a^3 \cdot a^{-1}((x \cdot ax) \cdot a^{-1}b) = a \cdot a(x \cdot a(x \cdot a^{-1}b))$, using (i) in the third equality. Cancelling a on the left and multiplying by x on the left, we have

$$x^3 \cdot ab = x \cdot a(x \cdot a(x \cdot a^{-1}b)) = (x \cdot (a \cdot xa)x) \cdot a^{-1}b. \tag{3.2}$$

Since $x \cdot (a \cdot xa)x = x \cdot a(x \cdot ax) = x \cdot a(x^2a) = x \cdot x^2a^2 = x^3a^2 = a \cdot x^3a$, we can rewrite (3.2) as $x^3 \cdot ab = (a \cdot x^3a) \cdot a^{-1}b = a \cdot x^3b = x^3b \cdot a$, and (ii) follows. □

Corollary 3.4. *Let Q be a Bol loop. For each positive integer n, $\langle C_{3n}(Q)\rangle$ is an abelian group, and $R|_{\langle C_{3n}(Q)\rangle} : \langle C_{3n}(Q)\rangle \to \mathrm{Mlt}(Q)$ is a homomorphism. If, in addition, Q is finite, then $|\langle C_{3n}(Q)\rangle|$ divides $|Q|$.*

Proof. By Lemma 3.3(i), $R_aR_b = R_{ab}$ for all $a, b \in C_{3n}(Q)$, and so Theorem 3.1 applies with $A = C_{3n}(Q)$. □

Corollary 3.5. *Let Q be a Bol loop such that $C(Q) = C_{3n}(Q)$ for some integer $n > 0$. Then $\langle C(Q)\rangle$ is an abelian group, and $R|_{\langle C(Q)\rangle} : \langle C(Q)\rangle \to \mathrm{Mlt}(Q)$ is a homomorphism. If, in addition, Q is finite, then $|\langle C(Q)\rangle|$ divides $|Q|$.*

Corollary 3.6. *Let Q be a finite Bol loop of order relatively prime to 3. Then $\langle C(Q)\rangle$ is an abelian group, $R|_{\langle C(Q)\rangle} : \langle C(Q)\rangle \to \mathrm{Mlt}(Q)$ is a homomorphism, and $|\langle C(Q)\rangle|$ divides $|Q|$.*

Note that one cannot replace right translations with left translations in Corollary 3.5, for otherwise $C(Q)$ would necessarily be a subloop.

Recall that any two elements of a Moufang loop generate a group, *i.e.*, Moufang loops are *diassociative.* It is well known that nonMoufang Bol loops are not diassociative. However, after seeing the calculations in the proof of Lemma 3.3, the reader might wonder if in a Bol loop, two elements generate a group if one of the two elements is in the commutant. The answer is “no”:

Example 3.7. Let Q be the Bol loop

	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	1	4	3	6	5	8	7
3	3	4	1	2	7	8	5	6
4	4	3	2	1	8	7	6	5
5	5	6	7	8	1	2	3	4
6	6	5	8	7	2	1	4	3
7	7	8	5	6	4	3	2	1
8	8	7	6	5	3	4	1	2

Then $Z(Q) = N_\lambda(Q) = \{1, 2\}$, $C(Q) = N_\rho(Q) = \{1, 2, 3, 4\}$, and $\langle 4, 5\rangle = Q$.

We do not know the answer to the following.

Problem 3.8. *Does there exist a finite Bol loop of order relatively prime to* 3 *such that the commutant is not contained in the right nucleus?*

4. Left Nuclear Extensions of Bol Loops

Let $(Q, \cdot)$, $(K, \cdot)$, $(E, *)$ be loops. Then Q is an *extension of K by E* if K is a normal subloop of Q and $Q/K = E$. We can then identify E with a subset of Q—in fact, with a transversal of Q/K—and assume without loss of generality that $1_E = 1_Q = 1$. Given a, $b \in E$, there is then a unique $f(a, b) \in K$ such that $ab = f(a, b)(a*b)$. The map $f : E \times E \to K$ thus obtained satisfies $f(a, 1) = f(1, a) = 1$. We will call a map with the property $f(a, 1) = f(1, a) = 1$ a *cocycle.*

Theorem 4.1. *Let $(K, \cdot)$, $(E, *)$ be loops, and Q an extension of K by E such that $K \le N_\lambda(Q) \cap N_\mu(Q)$. Then K is a group, there is a map $f : E \times E \to K$ satisfying $f(1, a) = f(a, 1) = 1$, and a map $\tau : E \to \mathrm{Aut}(K)$ satisfying $\tau_1 = 1$, such that Q is isomorphic to $K \times E$ with multiplication*

$$(u, a)(v, b) = (u\tau_a(v)f(a, b), a * b) \tag{4.1}$$

for every a, $b \in E$, u, $v \in K$.

Conversely, given a group $(K, \cdot)$, a loop $(E, *)$, a cocycle $f : E \times E \to K$, and a map $\tau : E \to \mathrm{Aut}(K)$ with $\tau_1 = 1$, the loop $Q = K \times E$ with multiplication (4.1) *is an extension of K by E, and $K \le N_\lambda(Q) \cap N_\mu(Q)$.*

Proof. K is obviously a group since it is a subloop of two nuclei. Let $f : K \times K \to E$ be the cocycle described above. For $a \in E$, let $\tau_a : K \to K$ by defined by $\tau_a(u)a = au$ for every $u \in K$. Since τ_a is the restriction of the inner mapping $L_aR_a^{-1}$ of Q to K, and since K is normal in Q, τ_a is a bijection of K.

We claim that τ_a is a homomorphism. We have $\tau_a(uv) = \tau_a(u)\tau_a(v)$ if and only if $\tau_a(uv)a = \tau_a(u)\tau_a(v) \cdot a = \tau_a(u) \cdot \tau_a(v)a$ (since $K \le N_\lambda(Q)$) if and only if $a(uv) = \tau_a(u) \cdot av$ if and only if $a \cdot uv = \tau_a(u)a \cdot v = au \cdot v$ (again by $K \le N_\lambda(Q)$). But $a \cdot uv = au \cdot v$, since $u \in N_\mu(Q)$. Thus τ_a is a homomorphism, and $\tau : a \mapsto \tau_a$ is a map $E \to \mathrm{Aut}(K)$. We see right away that $\tau_1 = 1$.

Every element of Q can be expressed uniquely as ua, where $u \in K$ and $a \in E$ (since E is a transversal of Q/K). For $u, v \in K$, $a, b \in E$, we have: $ua \cdot vb = u(a \cdot vb)$ (since $u \in K \leq N_\lambda(Q)$), $u(a \cdot vb) = u(av \cdot b)$ (since $v \in K \leq N_\mu(Q)$). As $\tau_a(v) \in K$ and $f(a,b) \in K$, we have $u(av \cdot b) = u(\tau_a(v)a \cdot b) = u(\tau_a(v) \cdot ab) = u\tau_a(v) \cdot ab = u\tau_a(v) \cdot f(a,b)(a * b) = u\tau_a(v)f(a,b) \cdot (a * b)$.

For the converse, it is easy to see that $Q = K \times E$ with multiplication (4.1) is a loop, $K \trianglelefteq Q$, and $Q/K = E$. We have

$$\begin{aligned}(u,1)(v,b) \cdot (w,c) &= (uv\tau_b(w)f(b,c), bc) = (u,1) \cdot (v,b)(w,c), \text{ and}\\ (v,b)(u,1) \cdot (w,c) &= (v\tau_b(u)\tau_b(w)f(b,c), bc) = (v\tau_b(uw)f(b,c), bc)\\ &= (v,b) \cdot (u,1)(w,c),\end{aligned}$$

and hence $K \leq N_\lambda(Q) \cap N_\mu(Q)$. □

Since the left and middle nuclei coincide in Bol loops, we have the following.

Corollary 4.2. *Let K be a group, E a Bol loop. Assume that Q is a Bol loop which is an extension of K by E, and that $K \leq N_\lambda(Q)$. Then the multiplication in Q is given by* (4.1) *for some cocycle f and a map $\tau : E \to \mathrm{Aut}(K)$ satisfying $\tau_1 = 1$.*

Denote the extension of K by E constructed as in (4.1) by $Q = Q(K, E, \tau, f)$. We are now going to give conditions on f and τ that make Q into a Bol loop.

Theorem 4.3. *Let K be a group, E a Bol loop, $f : E \times E \to K$ a cocycle and $\tau : E \to \mathrm{Aut}(K)$ a map satisfying $\tau_1 = 1$, and set $Q = Q(K, E, \tau, f)$. Then:*

(i) *Q is a Bol loop if and only if*

$$\tau_a(f(b,a))f(a,ba)f(a \cdot ba, c) = \tau_a\tau_b(f(a,c))\tau_a(f(b,ac))f(a, b \cdot ac), \tag{4.2}$$

$$\tau_a(f(b,a))f(a,ba)\tau_{a \cdot ba}(w) = \tau_a\tau_b\tau_a(w)\tau_a(f(b,a))f(a,ba) \tag{4.3}$$

for every $w \in K$ and $a, b, c \in E$.

(ii) *$(w,c) \in Q$ belongs to $N_\rho(Q)$ if and only if $c \in N_\rho(E)$ and*

$$f(a,b)\tau_{ab}(w)f(ab,c) = \tau_a\tau_b(w)\tau_a(f(b,c))f(a,bc) \tag{4.4}$$

for all $a, b \in E$.

(iii) *Q is a group if and only if E is a group and*

$$\tau_a(f(b,c))f(a,bc) = f(a,b)f(ab,c), \tag{4.5}$$

$$\tau_a\tau_b(w)f(a,b) = f(a,b)\tau_{ab}(w) \tag{4.6}$$

for every $w \in K$ and $a, b, c \in E$.

(iv) *$(u,a) \in Q$ belongs to $C(Q)$ if and only if $a \in C(E)$ and*

$$\tau_a(v) = u^{-1}vu \tag{4.7}$$

$$\tau_b(u) = uf(a,b)f(b,a)^{-1} \tag{4.8}$$

for every $v \in K$, $b \in E$.

Proof. For (i): By straightforward calculation with $x = (u,a)$, $y = (v,b)$, $z = (w,c)$ substituted into the Bol identity $(x \cdot yx)z = x(y \cdot xz)$, we obtain that Q is a Bol loop if and only if

$$\tau_a(f(b,a))f(a,ba)\tau_{a \cdot ba}(w)f(a \cdot ba, c) = \tau_a\tau_b\tau_a(w)\tau_a\tau_b(f(a,c))\tau_a(f(b,ac))f(a, b \cdot ac) \tag{4.9}$$

for all $w \in K$ and $a, b, c \in E$. Taking $w = 1$ gives (4.2), while taking $c = 1$ gives (4.3). Conversely, it is easy to see that if both (4.2) and (4.3) hold, then (4.9) holds.

For (ii), we merely substitute $x = (u, a)$, $y = (v, b)$, and $z = (w, c)$ into the associative law $x \cdot yz = xy \cdot z$. For (iii), then, it follows that Q is a group if and only if E is a group and (4.4) holds for all $a, b, c \in E$, $w \in K$. That (4.4), universally quantified, is equivalent to (4.5) and (4.6) is proven similarly as in (i).

For part (iv), we plug $x = (u, a)$, $y = (v, b)$ into the commutative law $xy = yx$ to get that $(u, a) \in C(Q)$ if and only if $a \in C(E)$ and

$$v\tau_b(u)f(b, a) = u\tau_a(v)f(a, b) \tag{4.10}$$

for all $v \in K$, $b \in E$. Taking $b = 1$ and rearranging gives (4.7), while taking $v = 1$ and rearranging gives (4.8). Conversely, it is easy to see that if both (4.7) and (4.8) hold, then (4.10) holds. □

In the next two sections, we will consider two special cases. The extension $Q(K, E, \tau, f)$ is a *semidirect product* if $f : E \times E \to K$ satisfies $f(a, b) = 1$ for every a, $b \in E$. In such a case, we denote the resulting loop by $Q(K, E, \tau)$. Semidirect products of Bol loops were considered in [4].

When A, B are loops, a map $\varphi : A \to B$ is a *semihomomorphism* if $\varphi(a \cdot ba) = \varphi(a) \cdot \varphi(b)\varphi(a)$ for every a, $b \in A$.

Corollary 4.4. *Let K be a group, E a Bol loop, and $\tau : E \to \mathrm{Aut}(K)$ a map satisfying $\tau_1 = 1$, and set $Q = Q(K, E, \tau)$. Then:*

(i) *Q is a Bol loop if and only if τ is a semihomomorphism.*
(ii) *$(w, c) \in Q$ belongs to $N_\rho(Q)$ if and only if $c \in N_\rho(E)$ and $\tau_{ab}(w) = \tau_a\tau_b(w)$ for all $a, b \in E$.*
(iii) *Q is a group if and only if E is a group and τ is a homomorphism.*
(iv) *$(u, a) \in Q$ belongs to $C(Q)$ if and only if $a \in C(E)$, $\tau_a(v) = u^{-1}vu$ for every $v \in K$, and $u = \tau_b(u)$ for every $b \in E$.*
(v) *$C(Q) \subseteq N_\rho(Q)$ if and only if $C(E) \subseteq N_\rho(E)$.*

Proof. Parts (i), (ii), (iii), and (iv) follow immediately from specializing the corresponding parts of Theorem 4.3. For (v), if $(w, c) \in C(Q)$, then by (iv), we trivially have $\tau_{ab}(w) = \tau_a\tau_b(w)$ for all $a, b \in E$. If $C(E) \subseteq N_\rho(E)$, then $c \in N_\rho(E)$, and so $(w, c) \in N_\rho(Q)$ by (ii). Conversely, if $C(Q) \subseteq N_\rho(Q)$, then for $c \in C(E)$, $(1, c) \in N_\rho(Q)$, and so $c \in N_\rho(E)$ by (ii). □

For $f \in \mathrm{Aut}(K)$, let $\mathrm{Fix}(f) = \{u \in K \,|\, f(u) = u\}$. For a map $\tau : E \to \mathrm{Aut}(K)$, let $\mathrm{Ker}(\tau) = \{e \in E \,|\, \tau_e = 1\}$ and $\mathrm{Fix}(\tau) = \{u \in K \,|\, u \in \mathrm{Fix}(\tau_e)$ for every $e \in E\}$.

Corollary 4.5. *Let E, K, τ and $Q = Q(K, E, \tau)$ be as in Corollary 4.4. If both E and K are commutative, then $C(Q) = \{(u, a) \,|\, u \in \mathrm{Fix}(\tau)$ and $a \in \mathrm{Ker}(\tau)\}$ and $|C(Q)| = |\mathrm{Fix}(\tau)| \cdot |\mathrm{Ker}(\tau)|$.*

The other special case of Theorem 4.3 we consider is where the "action" $\tau : E \to \mathrm{Aut}(K)$ is trivial. Denote by ι the map $\iota : E \to \mathrm{Aut}(K); a \mapsto 1$.

Corollary 4.6. *Let K be a group, E a Bol loop, $f : E \times E \to K$ a cocycle, and set $Q = Q(K, E, \iota, f)$. Then:*

(i) *Q is a Bol loop if and only if $f(b,a)f(a,ba) \in Z(K)$ and*

$$f(b,a)f(a,ba)f(a\cdot ba,c) = f(a,c)f(b,ac)f(a,b\cdot ac) \tag{4.11}$$

for every a, b, $c \in E$.

(ii) *$(w,c) \in Q$ belongs to $N_\rho(Q)$ if and only if $c \in N_\rho(E)$ and*

$$w^{-1}f(a,b)wf(ab,c) = f(b,c)f(a,bc) \tag{4.12}$$

for all $a, b \in E$.

(iii) *Q is a group if and only if E is a group, $f(a,b) \in Z(K)$, and*

$$f(b,c)f(a,bc) = f(a,b)f(ab,c) \tag{4.13}$$

for every a, b, $c \in E$.

(iv) *$(u,a) \in Q$ belongs to $C(Q)$ if and only if $a \in C(E)$, $u \in Z(K)$, and $f(a,b) = f(b,a)$ for every $b \in E$.*

Proof. These claims follow immediately from specializing the corresponding parts of Theorem 4.3. □

5. Constructions based on semidirect products

Moorhouse classified all nonassociative right Bol loops of order 16, viz [12]. It turns out that among these 2049 loops precisely 21 have a non-subloop commutant: 1 of order 12, and 20 of order 16. Among the 20 loops of order 16, 19 loops have commutant of order 6, and 1 loop has commutant of order 4.

We show in this subsection that precisely 3 of the 21 loops can be obtained by a semidirect construction. All 21 loops will be constructed in the next section.

Proposition 5.1. *Let K be a group, E an elementary abelian 2-group, $\tau : E \to \mathrm{Aut}(K)$ a map such that $\tau_1 = 1$, $|\tau_e| = 2$ for every e, and $\langle \tau_E \rangle$ is a commutative subgroup of $\mathrm{Aut}(K)$. Assume further that there are a, $b \in E$ such that $\tau_a = \tau_b = 1 \neq \tau_{ab}$. Then:*

(i) *τ is a semihomomorphism but not a homomorphism,*

(ii) *$Q = Q(K,E,\tau)$ is a nonassociative Bol loop,*

(iii) *$C(Q)$ is not a subloop of Q,*

(iv) *$C(Q) \subseteq N_\rho(Q)$.*

Proof. We have $\tau_{a\cdot ba} = \tau_b$ since E is an elementary abelian 2-group. On the other hand, $\tau_a \cdot \tau_b\tau_a = \tau_b$ since $\langle \tau_E \rangle$ is commutative and τ_a is an involution. The condition $\tau_a = \tau_b = 1 \neq \tau_{ab}$ guarantees that τ is not a homomorphism. This proves (i). Then (ii) follows by Corollary 4.4. Given a, $b \in E$ such that $\tau_a = \tau_b = 1 \neq \tau_{ab}$, note that $(1,a)$, $(1,b)$ belong to $C(Q)$ but $(1,ab)$ does not, and so (iii) holds. Finally, (iv) follows from Corollary 4.4(v) since E is a group. □

Example 5.2. Let $E = \langle e_1, e_2 \rangle$ be the elementary abelian 2-group of order 4, and K the cyclic group of order 3, $\mathrm{Aut}(K) = \{1, \varphi\}$. Define $\tau : E \to \mathrm{Aut}(K)$ by $\tau_1 = \tau_{e_1} = \tau_{e_2} = 1$, $\tau_{e_1e_2} = \varphi$. Then $|\mathrm{Ker}(\tau)| = 3$, $|\mathrm{Fix}(\tau)| = |\mathrm{Fix}(\varphi)| = 1$. Hence $Q = Q(K,E,\tau)$ is a nonassociative Bol loop of order 12 with non-subloop commutant of order 3.

Example 5.3. Let $E = \langle e_1, e_2\rangle$ be the elementary abelian 2-group of order 4, and K the cyclic group of order 4, $\mathrm{Aut}(K) = \{1, \psi\}$. Define $\tau : E \to \mathrm{Aut}(K)$ by $\tau_1 = \tau_{e_1} = \tau_{e_2} = 1$, $\tau_{e_1e_2} = \psi$. Then $|\mathrm{Ker}(\tau)| = 3$, $|\mathrm{Fix}(\tau)| = |\mathrm{Fix}(\psi)| = 2$. Hence $Q = Q(K, E, \tau)$ is a nonassociative Bol loop of order 16 with non-subloop commutant of order 6. It is easy to check that Q contains 9 involutions.

Example 5.4. Assume that both $E = \langle e_1, e_2\rangle$ and $K = \langle k_1, k_2\rangle$ are elementary abelian 2-groups of order 4. Define $\tau : E \to \mathrm{Aut}(K)$ by $\tau_1 = \tau_{e_1} = \tau_{e_2} = 1$, $\tau_{e_1e_2} : k_1 \mapsto k_1,\ k_2 \mapsto k_1k_2$. Then $|\mathrm{Ker}(\tau)| = 3$, $|\mathrm{Fix}(\tau)| = |\mathrm{Fix}(\tau_{e_1e_2})| = 2$. Hence $Q = Q(K, E, \tau)$ is a nonassociative Bol loop of order 16 with non-subloop commutant of order 6. It is easy to check that Q contains 13 involutions.

Lemma 5.5. *Let E, K, τ be as in Corollary 4.4. If $|E| = 2$ or $|K| = 2$ then $Q(K, E, \tau)$ is a group if and only if it is a Bol loop.*

Proof. Let $E = \{1, e\}$, and assume that τ is a semihomomorphism. Then $\tau_e = \tau_{eee} = \tau_e\tau_e\tau_e$ implies $\tau_{ee} = 1 = \tau_e\tau_e$, and hence τ is a homomorphism.

If $|K| = 2$ then $\mathrm{Aut}(K) = \{1\}$ and τ is a homomorphism. □

Lemma 5.6. *Of the known Bol loops of order at most 16 with non-subloop commutant, those constructed in Examples 5.2, 5.3, 5.4 are the only ones obtained by a nontrivial ($|E| > 1$ and $|K| > 1$) application of the semidirect construction of Corollary 4.4.*

Proof. We rely on Moorhouse's classification [12]; the caveat "known" in the statement of the lemma is because the classification of the Bol loops of order 16 has not been independently verified. By Corollary 2.9, the only possible orders less than or equal to 16 for Bol loops with non-subloop commutants are 8, 12, and 16. None of the Bol loops of order 8 have non-subloop commutant. (This also follows from Burn's classification of Bol loops of order 8 [2].)

The loop of Example 5.2 is the only Bol loop of order 12 with non-subloop commutant, by the classification. (This also follows from Burn's classification of Bol loops of order $4p$, p an odd prime [3].)

Assume that $Q = Q(K, E, \tau)$ is a Bol loop of order 16 with non-subloop commutant. By Lemma 5.5, we can assume that $|E| = 4$ and $|K| = 4$. Let $k = |\mathrm{Ker}(\tau)|$, $f = |\mathrm{Fix}(\tau)|$. Since both E and K are abelian, $|C(Q)| = kf$ by Corollary 4.5. By the classification, the only possible values of $|C(Q)|$ are 4 and 6. If $k = 4$ or $f = 4$, $\tau_e = 1$ for every $e \in E$ and hence τ is a homomorphism, a contradiction.

If K is cyclic, we have $f = 2$ iff there is $e \in E$ such that τ_e is the unique involution of $\mathrm{Aut}(\mathbb{Z}_4)$. If K is elementary abelian, we have $\mathrm{Aut}(K) \cong S_3$, and hence $f = 2$ if and only if all non-identity automorphism τ_e are equal to the same involution of $\mathrm{Aut}(K)$.

Assume $|C(Q)| = 4$. Then $k = f = 2$. If $E = \langle e_1, e_2\rangle$ is elementary abelian, we can assume that $\tau_1 = \tau_{e_1} = 1$ and $1 \neq \tau_{e_2} = \tau_{e_1e_2}$ is an involution. But then τ is a homomorphism, a contradiction. If $E = \langle e\rangle$ is cyclic, then we can assume that either $\tau_1 = \tau_e = 1$ and $1 \neq \tau_{e^2} = \tau_{e^3}$ is an involution, which results in $1 \neq \tau_{e^3}\tau_{e^2}\tau_{e^3} = \tau_{e^3e^2e^3} = \tau_1 = 1$; or we can assume that $\tau_1 = \tau_{e^2} = 1$ and $1 \neq \tau_e = \tau_{e^3}$ is an involution, which means that τ is a homomorphism.

Now assume that $|C(Q)| = 6$. Then $k = 3$, $f = 2$. If $E = \langle e_1, e_2\rangle$ is elementary abelian, we can assume that $1 = \tau_{e_1} = \tau_{e_2}$ and $1 \neq \tau_{e_1e_2}$ is an involution. Since there is a unique involution in $\mathrm{Aut}(\mathbb{Z}_4)$ and since $\mathrm{Aut}(\mathrm{Aut(K)}) \cong S_3$ acts transitively on the involutions of $\mathrm{Aut(K)} \cong S_3$ when K is elementary abelian, this case yields the loops obtained in Examples 5.3 and 5.4. Finally assume that $E = \langle e\rangle$ is cyclic. Then we can assume that either $\tau_e = \tau_{e^2} = 1$ and $1 \neq \tau_{e^3}$ is an involution, which yields $1 \neq \tau_{e^3} = \tau_{eee} = \tau_e\tau_e\tau_e = 1$; or we can assume that $\tau_e = \tau_{e^3} = 1 \neq \tau_{e^2}$, which yields $1 \neq \tau_{e^2} = \tau_e\tau_{e^2}\tau_e = \tau_{ee^2e} = 1$, a contradiction. □

Note that if the commutant $C(Q)$ of a Bol loop Q has order 2, say, $C(Q) = \{1, a\}$, then $C(Q)$ is a subloop. By contrast, we have the following.

Proposition 5.7. *For each $k > 2$, there exists a Bol loop with non-subloop commutant of order k.*

Proof. Pick n such that $2^n > k$. Let E be the elementary abelian 2-group of order 2^n, and let K be the cyclic group of order 3, thus $\mathrm{Aut}(K) = \{1, \varphi\}$. For some $a \neq 1 \neq b \neq a$ in E, let $\tau_1 = \tau_a = \tau_b = 1$, $\tau_{ab} = \varphi$. Choose the remaining $2^n - 4$ automorphisms τ_e of K arbitrarily, but in such a way that $|\mathrm{Ker}(\tau)| = k$. Then $Q = Q(K, E, \tau)$ is a nonassociative Bol loop by Proposition 5.1. Moreover, since $|\mathrm{Fix}(\tau)| = |\mathrm{Fix}(\varphi)| = 1$ and both E and K are abelian, $|C(Q)| = k$ by Corollary 4.5. □

Proposition 5.8. *For each $n > 2$, there exists a Bol loop of order $4n$ with non-subloop commutant.*

Proof. Let $E = \langle e_1, e_2\rangle$ be the elementary abelian group of order 4, and let K be the cyclic group of order n. Then $\psi : k \mapsto k^{-1}$ is a non-identity involutory automorphism of K. Set $\tau_1 = \tau_{e_1} = \tau_{e_2} = 1$, $\tau_{e_1e_2} = \psi$. By Proposition 5.1, $Q = Q(K, E, \tau)$ is a nonassociative Bol loop of order $4n$ with non-subloop commutant. □

6. Constructions based on extensions

In this section, we will use additive notation for abelian groups. As an immediate consequence of Corollary 4.6 we get:

Lemma 6.1. *Let K be an abelian group, E be a group, $f : E \times E \to K$ a cocycle, and $Q = Q(K, E, \iota, f)$. Then:*

(i) *$(w, c) \in Q$ belongs to $N_\rho(Q)$ if and only if $f(a, b)+f(ab, c) = f(b, c)+f(a, bc)$ for all $a, b \in E$,*

(ii) *$(u, a) \in Q$ belongs to $C(Q)$ if and only if $f(a, b) = f(b, a)$ for every $b \in E$.*

Lemma 6.2. *Let E and K be elementary abelian 2-groups, $f : E \times E \to K$ a cocycle, and $Q = Q(K, E, \iota, f)$. Then:*

(i) *Q is a Bol loop if and only if*

$$f(a, a + c) = f(a, a) + f(a, c), \tag{6.1}$$

$$f(a, b + c) + f(a, b) + f(a, c) = f(b, a + c) + f(b, a) + f(b, c) \tag{6.2}$$

for all $a, b, c \in E$.

(ii) *If there exist $a, b, c \in E$ such that $f(a+b, c) \neq f(c, a+b)$ and $f(a,d) = f(d,a)$, $f(b,d) = f(d,b)$ for every $d \in E$, then $C(Q)$ is not a subloop of Q.*

Proof. We freely use that E and K are of exponent 2. In additive notation, the cocycle identity (4.11) is

$$f(b,a) + f(a, b+a) + f(b,c) = f(a,c) + f(b, a+c) + f(a, b+a+c). \qquad (6.3)$$

Taking $b = a$, we get (6.1), and applying (6.1) to (6.3), we get (6.2). Conversely, it is easy to see that (6.1) and (6.2) imply (6.3). This establishes (i).

Assume that a, b, c are as in (ii). Then $(0,a)$, $(0,b)$ belong to $C(Q)$ by Lemma 6.1. By the same Lemma, $(0,a)(0,b) = (f(a,b), a+b)$ does not belong to $C(Q)$. □

In case E is an abelian group, we say that the cocycle $f : E \times E \to K$ is *right additive* if $f(a, b+c) = f(a,b) + f(a,c)$ for every $a, b, c \in E$.

Lemma 6.3. *Let E and K be elementary abelian 2-groups, $f : E \times E \to K$ a right additive cocycle, and $Q = Q(K, E, \iota, f)$. Then Q is a Bol loop, and*

(i) *$(w, c) \in Q$ belongs to $N_\rho(Q)$ if and only if the mapping $E \to K; a \mapsto f(a,c)$ is a homomorphism,*

(ii) *$C(Q) \subseteq N_\rho(Q)$.*

Proof. That Q is a Bol loop follows immediately from Lemma 6.2(ii) and right additivity. Again using right additivity, Lemma 6.1(i) reduces to $(w,c) \in N_\rho(Q)$ if and only if $f(a+b, c) = f(a,c) + f(b,c)$ for all $a, b \in E$, and this establishes (i). Finally, if $(w,c) \in C(Q)$, then by Lemma 6.1(ii) and right additivity, $f(a+b, c) = f(c, a+b) = f(c,a) + f(c,b) = f(a,c) + f(b,c)$ for all $a, b \in E$, and so $(w,c) \in N_\rho(Q)$ by (i). □

When $K = \{0,1\} \cong \mathbb{Z}_2$ and E is an elementary abelian 2-group, then E is a vector space over K and a cocycle $f : E \times E \to K$ is a form satisfying $f(0,a) = f(a,0) = 0$. As usual, we say that $g : E \times E \to K$ is *equivalent* to f if there is $\varphi \in \mathrm{Aut}(E)$ such that $f(a,b) = g(\varphi(a), \varphi(b))$ for every a, $b \in E$.

Lemma 6.4. *Let E be a vector space over $K = \{0,1\}$ with basis $B = \{e_1, \ldots, e_n\}$. Let $c : E \times B \to K$ be a map satisfying $c(0, e_i) = 0$ for every $1 \leq i \leq n$. Then there is a unique right additive cocycle $f : E \times E \to K$ such that $f(e, e_i) = c(e, e_i)$ for every $e \in E$, $e_i \in B$.*

Proof. The map $f(a, \_) : E \to K$, $a \mapsto f(a,e)$ is a homomorphism for every a if and only if f is right additive. □

In the situation of the previous Lemma, we say that f is *associated* with c.

Proposition 6.5. *Let E be a vector space over $K = \{0,1\}$ with basis $B = \{e_1, \ldots, e_n\}$. Let $c : E \times B \to K$ be a map satisfying $c(0, e_i) = 0$, $c(e_1, e_i) = c(e_i, e_1)$, $c(e_2, e_i) = c(e_i, e_2)$ for every $1 \leq i \leq n$, and $c(e_1 + e_2, e_3) \neq c(e_1, e_3) + c(e_2, e_3)$. Assume furthermore that c is such that the right additive cocycle $f_c = f : E \times E \to K$ associated with c satisfies $f(e_1, e) = f(e, e_1)$, $f(e_2, e) = f(e, e_2)$ for every $e \in E$. Then $Q = Q(K, E, \iota, f)$ is a Bol loop with non-subloop commutant.*

Moreover, if $g : E \times E \to K$ is a right additive cocycle satisfying the assumptions of Lemma 6.2(ii), then g is equivalent to f_c with some choice of c as above.

Proof. The conditions $c(e_1+e_2,e_3)\neq c(e_1,e_3)+c(e_2,e_3)$, $f(e,e_1)=f(e_1,e)$, and $f(e,e_2)=f(e_2,e)$ guarantee that $f(e_1+e_2,e_3)\neq f(e_1,e_3)+f(e_2,e_3)=f(e_3,e_1)+f(e_3,e_2)=f(e_3,e_1+e_2)$. Hence f satisfies the assumptions of Lemma 6.2(ii), and $Q=Q(K,E,\iota,f)$ is a Bol loop with non-subloop commutant.

Let $g:E\times E\to K$ be a right additive cocycle with a, b, $c\in E$ such that $g(a,d)=g(d,a)$, $g(b,d)=g(d,b)$ for every $d\in E$, and such that $g(a+b,c)\neq g(c,a+b)$. Then $g(a+b,c)\neq g(c,a)+g(c,b)=g(a,c)+g(b,c)$.

It is clear that neither a nor b nor c can be equal to 0, and that $a\neq b$. Moreover, $c\neq a$ (else $g(a+b,c)=g(a+b,a)=g(a,a+b)=g(a,a)+g(a,b)=g(a,a)+g(b,a)=g(a,c)+g(b,c)$), $c\neq b$ (by a similar argument), and $c\neq a+b$ (else $g(a+b,c)=g(c,a+b)$). Hence a, b, c are linearly independent, and there is an automorphism of E that maps (a,b,c) to (e_1,e_2,e_3). □

Corollary 6.6. *Let E, K, B, n, c and f be as in Proposition 6.5. Then we are free to choose $(2^n-4)(n-2)+3n-4$ of the values of c.*

Proof. We can choose $c(e_1,e_i)$ for every $1\leq i\leq n$. Then $c(e,e_1)$ is determined for every $e\in E$ by the condition $f(e,e_1)=f(e_1,e)$. We can then choose $c(e_2,e_i)$ for every $2\leq i\leq n$, hence determining $c(e,e_2)$ for every e by the condition $f(e,e_2)=f(e_2,e)$. Since $c(e_1+e_2,e_3)\neq c(e_1,e_3)+c(e_2,e_3)$, the value $c(e_1+e_2,e_3)$ is determined. But we can choose $c(e_1+e_2,e_i)$ for every $4\leq i\leq n$. Finally for e not in the subspace $\langle e_1,e_2\rangle$, we are free to choose $c(e,e_i)$ for every $3\leq i\leq n$. □

Example 6.7. Let $E=\langle e_1,e_2,e_3\rangle$ be a 3-dimensional vector space over $K=\{0,1\}$. According to Corollary 6.6, we are free to choose $(2^3-1)(3-2)+3\cdot 3-4=9$ values of $c:E\times\{e_1,e_2,e_3\}\to K$ in order to uniquely determine the associated right additive cocycle $f:E\times E\to K$ such that $Q=Q(K,E,\iota,f)$ is a Bol loop with non-subloop commutant.

These nine choices are as follows:

c	e_1	e_2	e_3
e_1	c_1	c_2	c_4
e_2	.	c_3	c_5
e_1+e_2	.	.	.
e_3	.	.	c_6
e_1+e_3	.	.	c_7
e_2+e_3	.	.	c_8
$e_1+e_2+e_3$	.	.	c_9

The resulting loop of order 16 will be denoted by $Q(c_1,c_2,c_3,c_4,c_5,c_6,c_7,c_8,c_9)$.

Proposition 6.8. *All Bol loops of order 16 with non-subloop commutant are isomorphic to the loop $Q(c_1,\cdots,c_9)$ with some choice of $c_1,\ \dots,\ c_9\in K=\{0,1\}$, except for one loop.*

Proof. We have verified by computer, using the package LOOPS [8], that the following 19 Bol loops are pairwise non-isomorphic:

$$\begin{array}{lll}
Q(0,0,0,0,0,0,0,0,0), & Q(0,0,0,0,0,0,0,0,1), & Q(0,0,0,0,0,0,0,1,1), \\
Q(0,0,0,0,0,0,1,1,0), & Q(0,0,0,0,0,0,1,1,1), & Q(0,0,0,0,0,1,1,1,1), \\
Q(0,0,1,0,0,0,0,0,0), & Q(0,0,1,0,0,0,0,0,1), & Q(0,0,1,0,0,0,0,1,1), \\
Q(0,0,1,0,0,0,1,0,0), & Q(0,0,1,0,0,0,1,0,1), & Q(0,0,1,0,0,0,1,1,0), \\
Q(0,0,1,0,0,1,1,0,0), & Q(1,0,1,0,0,0,0,0,0), & Q(1,0,1,0,0,0,0,0,1), \\
Q(1,0,1,0,0,0,0,1,0), & Q(1,0,1,0,0,0,0,1,1), & Q(1,0,1,0,0,0,1,1,0), \\
Q(1,0,1,0,0,1,0,0,1). & &
\end{array}$$

There is only one additional Bol loop with non-subloop commutant, according to Moorhouse's classification. □

Here is the unique Bol loop Q of order 16 with non-subloop commutant not obtained in Proposition 6.8:

	K				Ke_1				Ke_2				Ke_1e_2			
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
k_1	2	1	4	3	6	5	8	7	10	9	12	11	14	13	16	15
k_2	3	4	1	2	7	8	5	6	12	11	10	9	16	15	14	13
k_1k_2	4	3	2	1	8	7	6	5	11	12	9	10	15	16	13	14
Ke_1	5	6	7	8	1	2	3	4	13	14	15	16	9	10	11	12
	6	5	8	7	2	1	4	3	16	15	14	13	12	11	10	9
	7	8	5	6	3	4	1	2	15	16	13	14	11	12	9	10
	8	7	6	5	4	3	2	1	14	13	16	15	10	9	12	11
Ke_2	9	10	11	12	13	14	15	16	1	2	3	4	5	6	7	8
	10	9	12	11	14	13	16	15	2	1	4	3	6	5	8	7
	11	12	9	10	15	16	13	14	3	4	1	2	7	8	5	6
	12	11	10	9	16	15	14	13	4	3	2	1	8	7	6	5
Ke_1e_2	13	14	15	16	9	10	11	12	5	6	7	8	1	2	3	4
	14	13	16	15	10	9	12	11	6	5	8	7	2	1	4	3
	15	16	13	14	11	12	9	10	7	8	5	6	3	4	1	2
	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Note that $N_\lambda(Q) = Z(Q) = \{1\}$, $N_\rho(Q) = \{1,2,3,4,5,6,7,8\}$ is an elementary abelian 2-group, and $C(Q) = \{1,2,5,7\}$. Also note that $N_\rho(Q) = \langle C(Q)\rangle$.

The fact that $N_\lambda(Q)$ is trivial implies that Q cannot be obtained by any extension (4.1) of Theorem 4.1. In [6], Kiechle and Nagy developed a theory of extensions of involutory Bol loops, and constructed all involutory Bol loops of order 16, three of which happen to have a trivial center. Since our loop Q is involutory and has trivial center, it is one of the three loops mentioned in [6, Corollary 7].

We conclude this section with an explicit construction of Q. Let $K = \langle k_1, k_2\rangle$ and $E = \langle e_1, e_2\rangle$ be elementary abelian 2-groups of order 4. For every $(a,b) \in E \times E$ we define an automorphism $\psi_{a,b}$ of K. Namely: $\psi_{1,e_2} = \psi_{1,e_1e_2}$ satisfies $k_1 \mapsto k_1$, $k_2 \mapsto k_1k_2$, $\psi_{e_1,e_1} = \psi_{e_1,e_1e_2}$ satisfies $k_1 \mapsto k_1k_2$, $k_2 \mapsto k_2$, and all other automorphisms $\psi_{a,b}$ are trivial. Then Q is isomorphic to $K \times E$ with multiplication $(u,a)(v,b) = (\psi_{a,b}(u)v, ab)$, as is easily seen from the multiplication table of Q. (For the convenience of the reader, we have subdivided the multiplication table of

Q into subsquares corresponding to the cosets of K, labeled the cosets of K, and also labeled the elements in one of the cosets.)

7. Acknowledgement

Our investigations were aided by the automated reasoning tools OTTER [9] and Prover9 [10], and by the finite model builder Mace4 [11].

References

[1] R. H. Bruck, *A Survey of Binary Systems*, Springer, 1971.

[2] R.P. Burn, Finite Bol loops, *Math. Proc. Cambridge Philos. Soc.* **84** (1978), 377–385.

[3] R.P. Burn, Finite Bol loops II, *Math. Proc. Cambridge Philos. Soc.* **88** (1981), 445–455.

[4] E. G. Goodaire and D. A. Robinson, Semi-direct products and Bol loops, *Demonstratio Math.* **27** (1994), 573–588.

[5] H. Kiechle, *Theory of K-loops*, Lecture Notes in Mathematics **1778**, Springer, 2002.

[6] H. Kiechle and G. P. Nagy, On the extension of involutorial Bol loops, *Abh. Math. Sem. Univ. Hamburg* **72** (2002), 235–250.

[7] M. K. Kinyon and J. D. Phillips, Commutants of Bol loops of odd order, *Proc. Amer. Math. Soc.* **132** (2004), 617–619.

[8] G. P. Nagy and P. Vojtěchovský, *LOOPS: Computing with quasigroups and loops in GAP*, version 1.0.0, computational package for GAP; `http://www.math.du.edu/loops`

[9] W. W. McCune, *OTTER 3.3 Reference Manual and Guide*, Argonne National Laboratory Technical Memorandum ANL/MCS-TM-263, 2003; `http://www.mcs.anl.gov/AR/otter/`

[10] W. W. McCune, *Prover9*, automated reasoning software, Argonne National Laboratory, 2005; `http://www.mcs.anl.gov/AR/prover9/`

[11] W. W. McCune, *Mace 4.0 Reference Manual and Guide*, Argonne National Laboratory Technical Memorandum ANL/MCS-TM-264, 2003; `http://www.mcs.anl.gov/AR/mace4/`

[12] G. Eric Moorhouse, Bol Loops of Small Order; `http://www.uwyo.edu/moorhouse/pub/bol/index.html`

[13] H. O. Pflugfelder, *Quasigroups and Loops: Introduction*, Sigma Series in Pure Math. **8**, Heldermann, 1990.

[14] D. A. Robinson, Bol loops, *Trans. Amer. Math. Soc.* **123** (1966), 341–354.

Department of Mathematical Sciences, Indiana University South Bend, South Bend, IN 46634 USA
E-mail address: `mkinyon@iusb.edu`
URL: `http://mypage.iusb.edu/~mkinyon`

Department of Mathematics & Computer Science, Wabash College, Crawfordsville, IN 47933 USA
E-mail address: `phillipj@wabash.edu`
URL: `http://www.wabash.edu/depart/math/faculty.html#Phillips`

Department of Mathematics, University of Denver, 2360 S Gaylord St, Denver, CO 80208 USA
E-mail address: `petr@math.du.edu`
URL: `http://www.math.du.edu/~petr`